السلام عليكم ورحمة الله
اليوم ان شاء الله سنحاول دراسة أداة قوية نعم اخوانى أداة قوية
لأنـها أزالة أقوى الأدوات من طريقها
دور هده الأداة هو اعطاء تقرير شامل للجهاز من كل الجوانب
من تعريفات للجهاز وبرامج بداية التشغيل والتغييرات التى طرأت على الجهاز
نتيجة الاصابة بأحد الفيروسات و نتيجة الاستعما الخاطئ لأحد التطبيقات
أعتقد أنكم عرفتم هده الأداة؟؟

نعم اخوانى الأداة هي **Runscanner**
قبل وضع محاور لدرس
سنطرح عليكم سؤال مادا تعرفون عل هده الأداة؟؟

اخوانى نريد من جميع الأخوة تحميل الأداة أولا

من هنـــا

Download Runscanner

موقع الأداة

http://www.runscanner.net/

هده أهم المحاور التى سنتناولـها ان شاء الله

بخصوص هده الأداة

*1 تعريف أداة**Runscanner**

*2 تبين الخاصيات الجديدة التى أتت بها والتى امتازة بها على**hijackthis**

*3 توضيح لمادا لم نعتمدها لحد الأن بالقسم وتشبتنا ب**hijackthis**

*4 شرح لكيفية التعامل مع هده الاداة أولا كيفية اسخراج التقرير بصيغتين

و كيفية الفحص المباشر من الموقع وكل هدا يوجد فى الخاصية الاولى وهي**Beginner mode**

*5شرح خاصية **Expert mode** في هده الخاصية يوجد الكثير لتوضيح

*6التركيز على التقرير التنفيدي **run** لشرح كيفية رفع التقرير الى خبير ليتم تحليله

ثم اعادة ارساله للعضو ليقوم بحدف الأسطر التى حددها الخبير

*7شرح كيفية تعلم تحليل أسطر هده الاداة

تعريف شامل للأداة من موقعها الرسمي

اداة مجانية تقوم بفحص شامل للنظام والبرامج العاملة به وبرامج بدء التشغيل والتعريفات والخدمات ونقاط الاختطاف.

ويمكن استعمالها لاكتشاف التغييرات اللتي طرأت على النظام نتيجة الاصابة بملفات تجسس اوفايروسات او اخطاء بشرية من قبل المستخدمين انفسهم.

هذه الاداة العجيبة بها مزايا خرافية بمعنى الكلمة حسب موقع الشركة الرسمي

وعن تجارب معها بكل صراحة وسنعرضها لكم الان.

-عدد الاسطر بها غير محدود ويزيد مع كل تحديث للمنتج.

-تحليل مباشر للمالوير على المواقع المتخصصة.

-تتمتع بقاتل بروسيس قوي جدا.

-حفظ التقارير بصيغتين مختلفتين على هيئة مفكرة او ملف تشغيلي.

-فلترة قوية للملفات.

-محرر لملفات الهوست.

-استعادة الاسطر والقيم المحذوفة بكل بساطة.

-اصلاح وتنشيط متصفح الاكسبلورر.

-تحليل شهادة ومصداقية البرامج المثبته على انظمتنا.

-يوجد بها وضعين للاستخدام وضع للمبتدئين ووضع للخبراء.

-تحليل للقيم الخوارزمية الرقمية والتشفيرات على موقع.FILE ADVISOR

-تحليل التقارير على موقع.www.systemlookup.com

-رفع التقارير وتحليلها على موقع.www.VirusTotal.com

-تحليل الوحدات المحملة.

-فحص التقارير بموقع المنتج الرسمي.

-اصلاح قيم الريجيستري.

ولا ننسى اخوانى تحدير بخصوص هده الأداة

<u>يجب عدم استعمال الاداة بشكل فردى لان ذلك سيؤدى الى نتائج سلبية على نظامك</u>

<u>وانا اخلى مسئوليتى عن اى اجتهاد فردى دون استشارة فريق الخبراء.</u>

<u>من هنا الموقع الرسمى للاداة لمزيد من المعلومات</u>

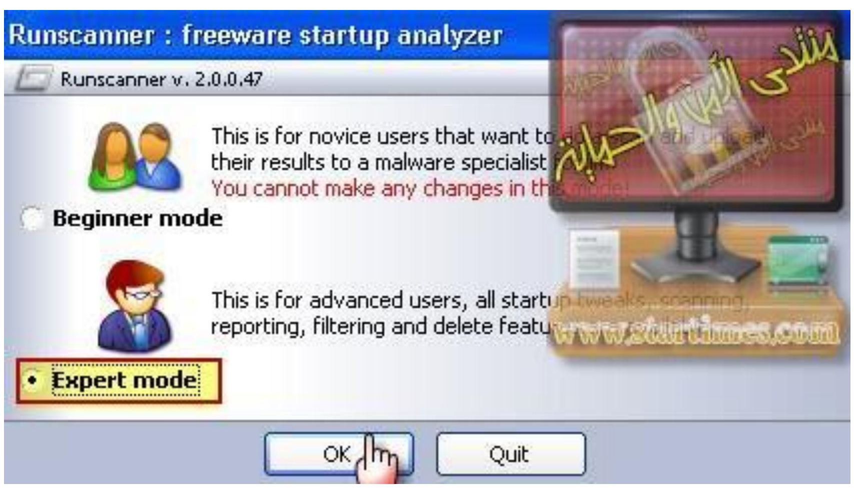
http://www.runscanner.net/

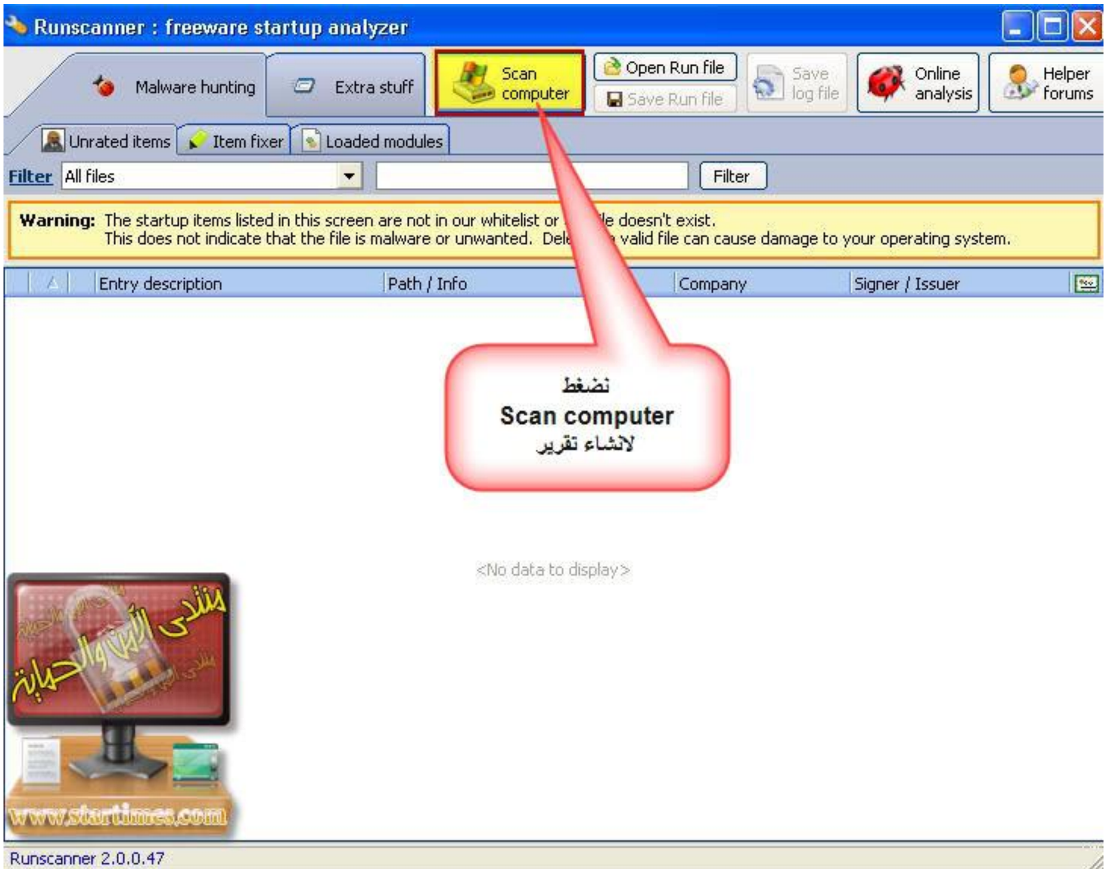
اخوانى الأداة بها 3 خاصيات للفحص
1الفحص عبر الموقع
2الفحص عبر الأداة
3الفحص من طرف الأخبراء
ودائما نجد تحديثات لها
والجميل ان التغيرات التى تطرء عليها نجدها بالموقع
من هنا
http://www.runscanner.net/changelog.aspx

كيفية انشاء التقرير اذا كنت تريد اراسله لحد الخبراء لحليله

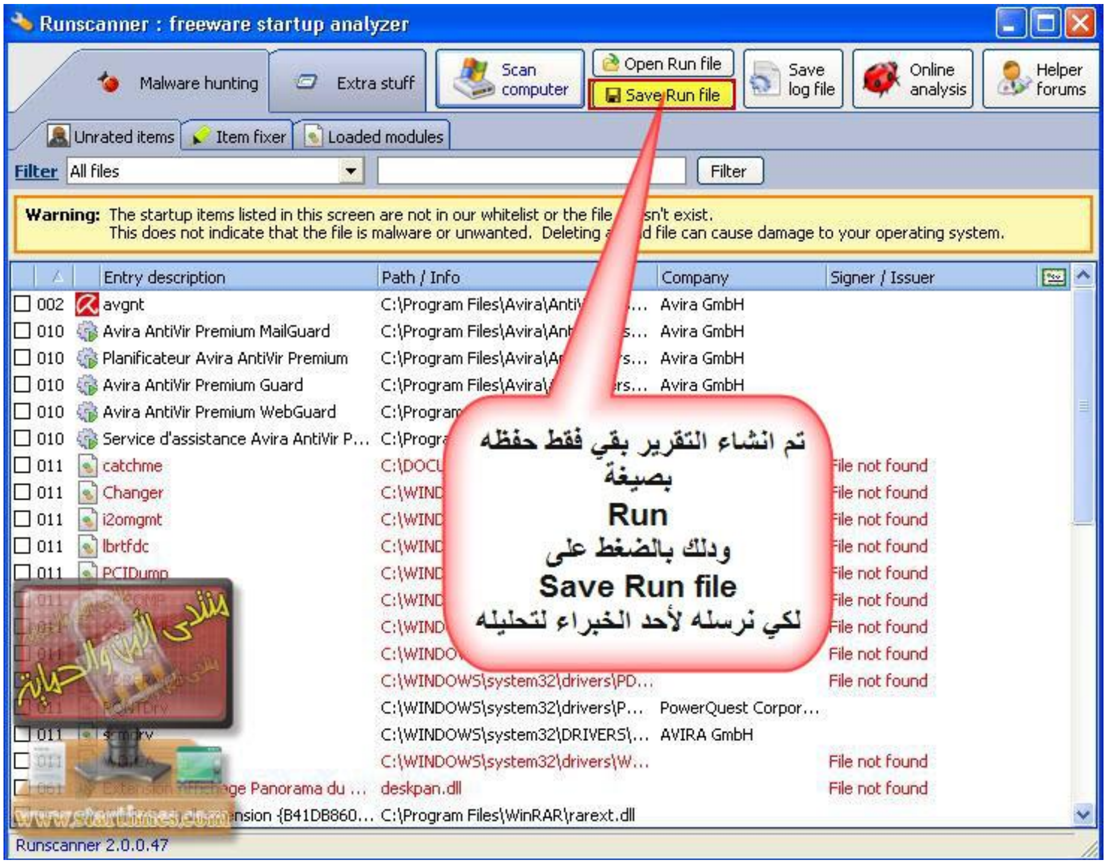
بعد الضغط على دوبل كليك على أيقونةRunscanner

نتقوم بتالى




Runscanner : freeware startup analyzer
Malware hunting
Extra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Helper forums
Unrated items
Item fixer
Loaded modules
Filter
All files
Filter
Entry description
Path / Info
Company
Signer / Issuer
نضغط
Scan computer
لانشاء تقرير
<No data to display>
www.startimes.com
Runscanner 2.0.0.47

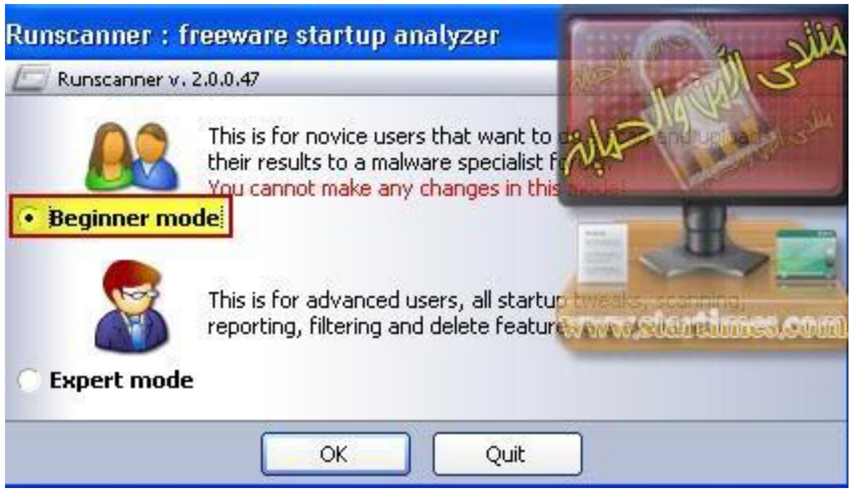

Runscanner scan in progress ...
جاري انشاء تقرير
Step 1: analysing loaded processes and dll libraries
Step 2: inventory of startup locations and hijack points
Step 3: calculating MD5 hashes and analysing digital signatures
Status : Analysing loaded processes and libraries
C:\WINDOWS\system32\USERENV.dll

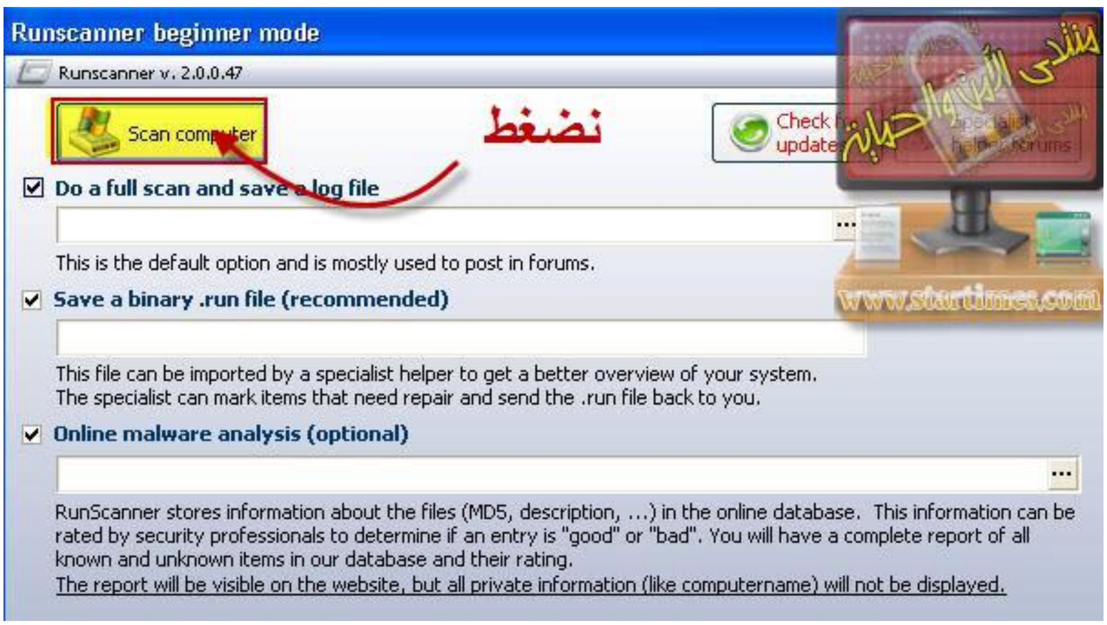




وهدا شرح لكيفية الحصول على التقرير للمبتدئين

وبتالى يمكنهم الفحص عبر الموقع


Runscanner : freeware startup analyzer
Runscanner v. 2.0.0.47
This is for novice users that want to
their results to a malware specialist f
You cannot make any changes in this
Beginner mode
This is for advanced users, all startup
reporting, filtering and delete featur
Expert mode
OK
Quit
www.startimes.com

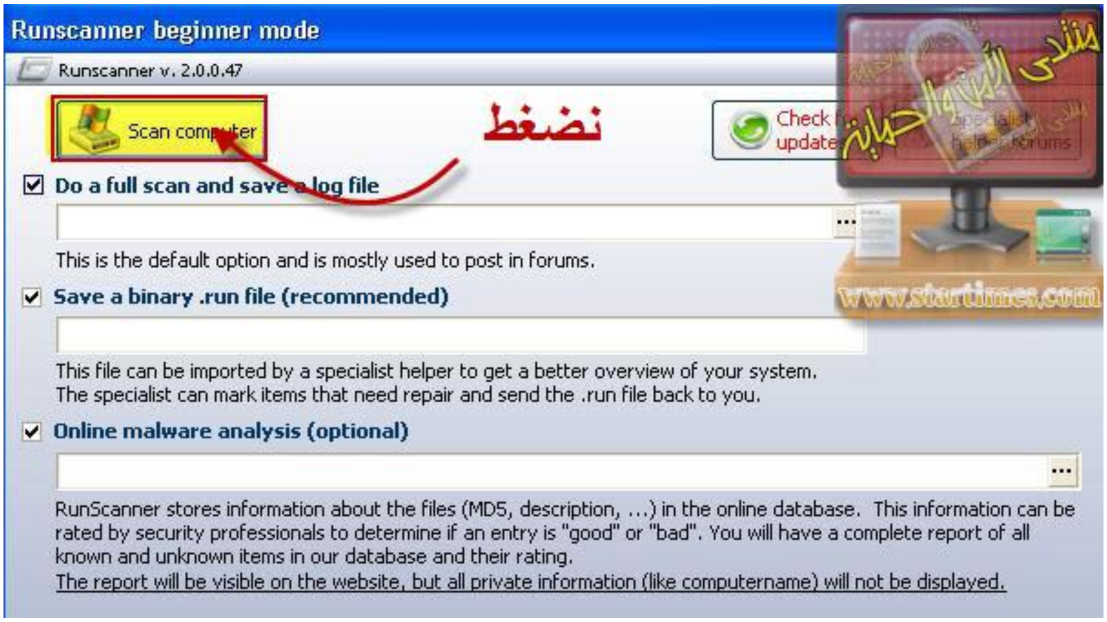

Runscanner beginner mode
Runscanner v. 2.0.0.47
Scan computer
نضغط
Do a full scan and save a log file
This is the default option and is mostly used to post in forums.
Save a binary .run file (recommended)
This file can be imported by a specialist helper to get a better overview of your system.
The specialist can mark items that need repair and send the .run file back to you.
Online malware analysis (optional)
RunScanner stores information about the files (MD5, description, ...) in the online database. This information can be rated by security professionals to determine if an entry is "good" or "bad". You will have a complete report of all known and unknown items in our database and their rating.
The report will be visible on the website, but all private information (like computername) will not be displayed.
www.startimes.com



هدا شرح

لكيفية تحليل التقرير عبر موقع الأداة





تم انشاء التقرير بجميع الخاصيات

هدفنا هو الفحص عبر الموقع لدى يجب ان

نضغط كما هو موضح فى الخاصية Online malware analysis3

ليتم تحويلنا مباشرة الى موقع الفحص



هدا هو موقع الفحص الأن يجب ان نبدأ بالفحص

ودلك بالاعتماد على الألوان

يوجد عندنا 3 ألوان

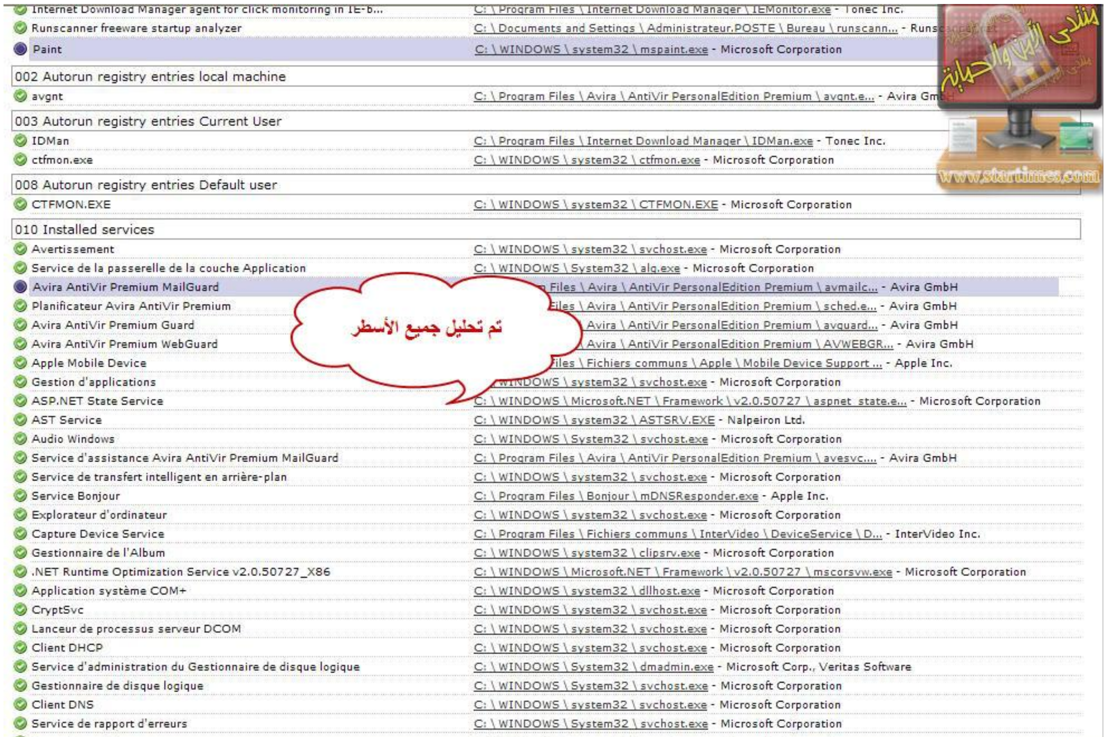
الأخضر وهو سليم

الأزرق لاتوجد له معلومات فى هدا الرابط لهدا يجب المزيد من الفحص عبر عدة خصائص

سنتعرف عليها فيما بعد

أما اللون الأحمر فهدا يعنى ان السطر ضار مباشرة للحدف





اخوانى فقط لتوضيح بعض الاشياء
ادا وجدنا فى المستطيل الملون بالأصفر

فقط لون أزرق ولون أحمر

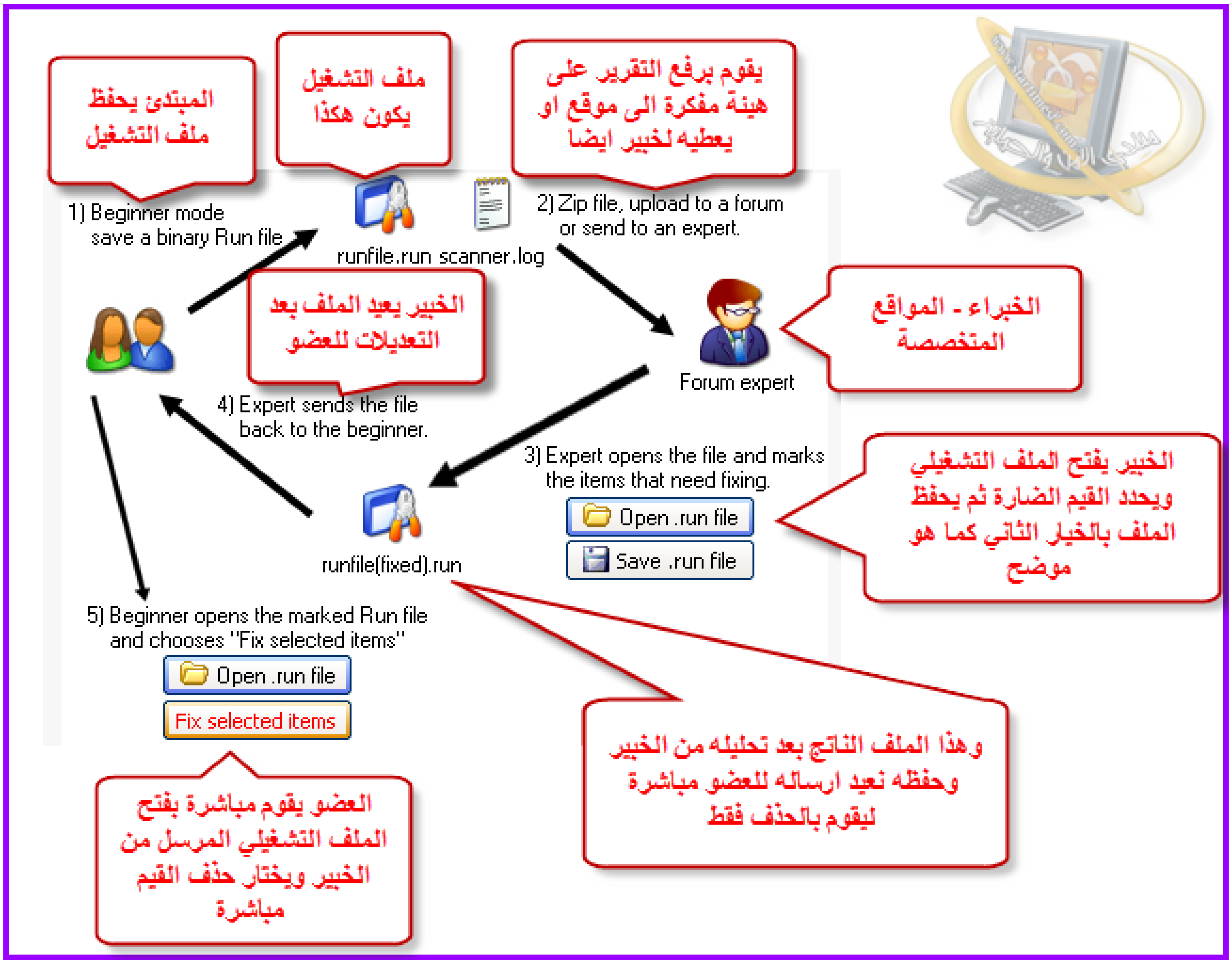
فهدا يعنى أن الأزرق سليم والأحمر ضار



فى انتظار التحاق الاخوة

يمكنكم مراجعة هدا الرسم الدى يوضح

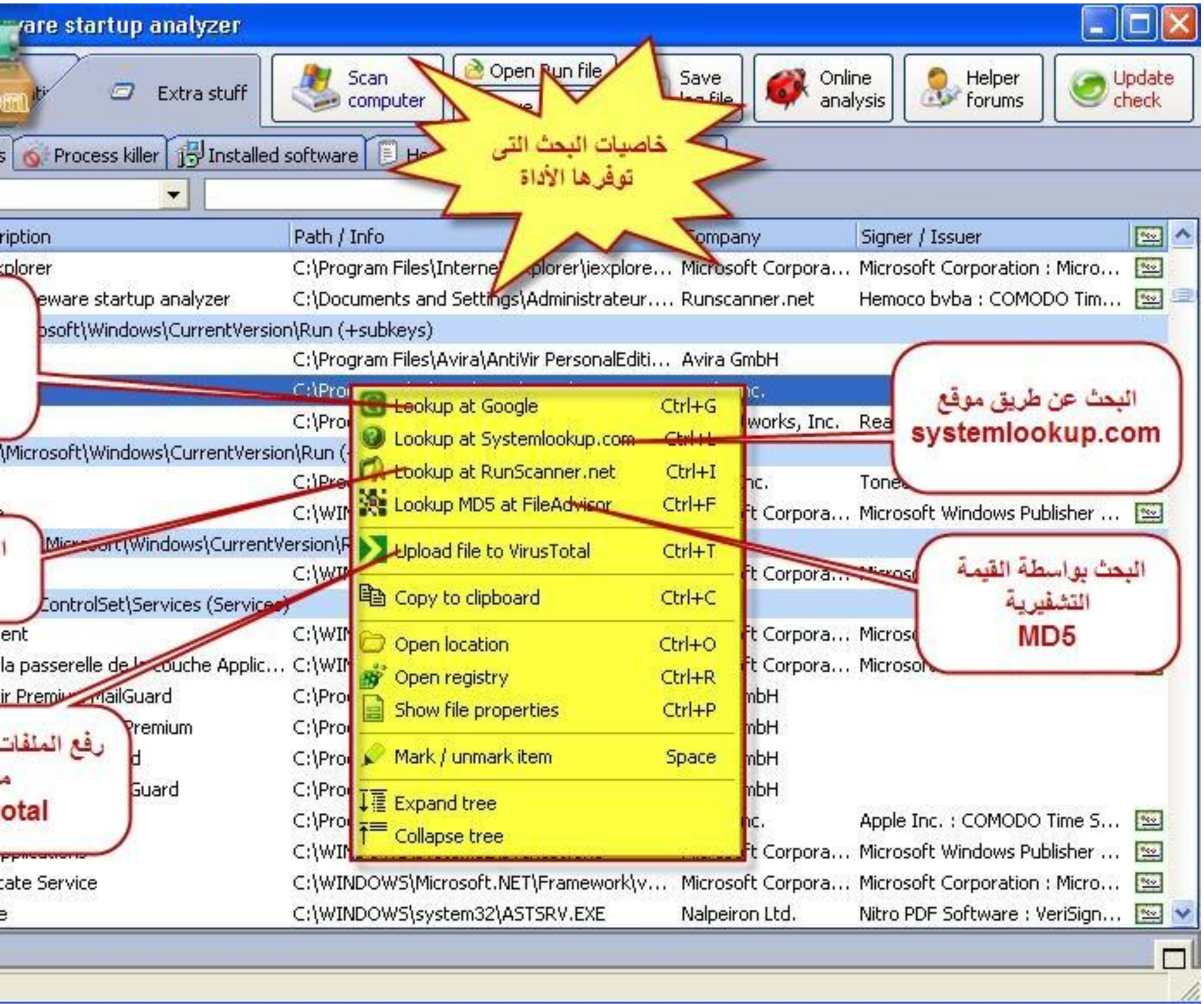
كيفية العمل بالاداة



كيفية تحليل أسطر هده الاداة سهل وأفضل منHijackthis

المشكل فقط هو في كثرة الأسطر أي تأخد منك الوقت الكثير رغم عمل فيلتر للأسطر

للتأكد من سلامة الاسطر فقط يجب الضغط بيمين الفأرة لكي يظهر لك كما في الصورة



أي يظهر لك

Lookup at google

Lookup at systemlookup.com

Lookup at Run scanner.net

Lookup MD5 at FileAdvisor

هده العناصر الثلاثة هي الخاصيات التي تقوم بفحص أسطر

الأول هو محرك البحث google وهو الافضل أي عندما تضغط عليه يتم تحويلك مباشرة اليه

وبتالى يعطيك مجموعة من النتائج لكي تتأكد هل السطر سليم ام ضار كما نقوم في Hijackthis نقوم بنسخ الجزء الأخير دات الامتداد exe أو... dll

ونضعه بمحرك البحث للحصول على نتائج وهو كدلك مع runscanner لا يوجد أي اختلاف لكن runscanner توفر عليك نسخ لصق

وتقوم بتحويلك مباشرة الى الموقع....

ونفس الشيئ بنسبة لى المواقع الأخر هي الأخرى بمجرد الضغط عليها تقوم بتحويلك مباشرة الى موقع الفحص للحصول على نتائج

التصنيف حسب الأكثر فعالية فى اعطاء نتائج صحيحة بين هده العناصر هو

1

google

2

الفحص بواسطة القيمة التشفيرية MD5

3

Runscanner.net

4
systemlookup.com
****
أما ادا لم تجد اجابة فى هده المواقع يمكنك رفع الملف المتمثل فى السطر تقوم برفعه على موقع virustotal لكي يتم فحصه واعطائك النتائج وهده الخاصية هي
Upload file to virus total

بنسبة للفحص بواسطة محرك البحث

أعتقد أنها مفهومة لا تستدعى الى شرح

سننتقل مباشرة الى الفحص بواسطة

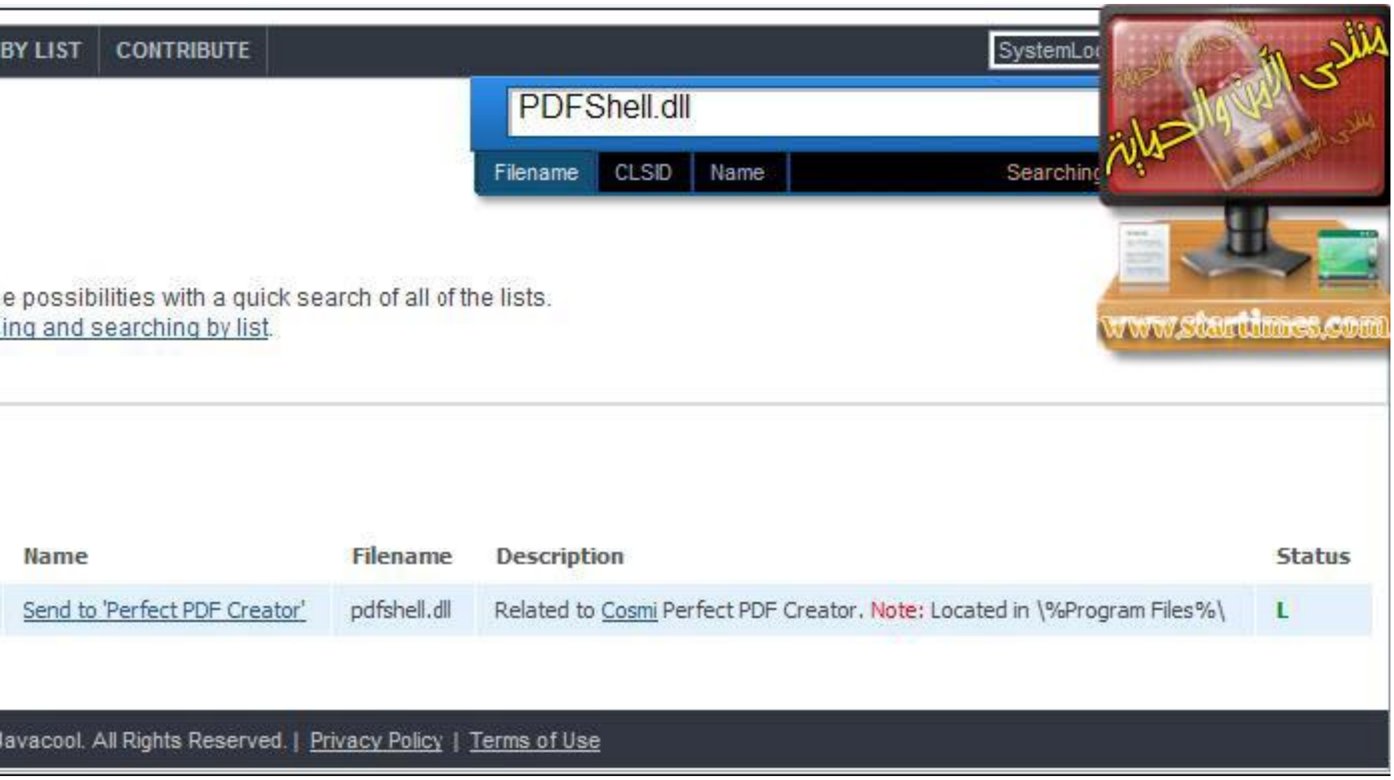
Lookup at systemlookup.com

عندما نضغط عليه يتم تحويلنا مباشرة الى الموقع

وهده صورة للموقع كيفية معرفة الأسطر السليمة من الضار

انظرو الى الحرف الأخير الملون بالأخضر الموجود بـStatus

هده الوضعية هي التى تحدد الاسطر السليمة من الضارة



عندما نريد فحص عبر هدا الموقع

سنجد هده الأحرف

الصنف الأول وهو خاص بالبرامج التى تقلع مع تشغيل الونداوز

وهي

Y

N

U

X

?

الصنف التنى من الأسطر وهي خاصة ببافى التطبيقات

وهي

X

L

O

?

شرح الأحرف

Xمباشرة للحدف

Lسطر سليم

Oلك الاختيار فى حدفه او تركه هنا وجب المزيد من التأكد

?غير معروف هو الأخر يجب ان نتأكد منه عبر باقى المواقع

الأن ننتقل الى الخاصية 3

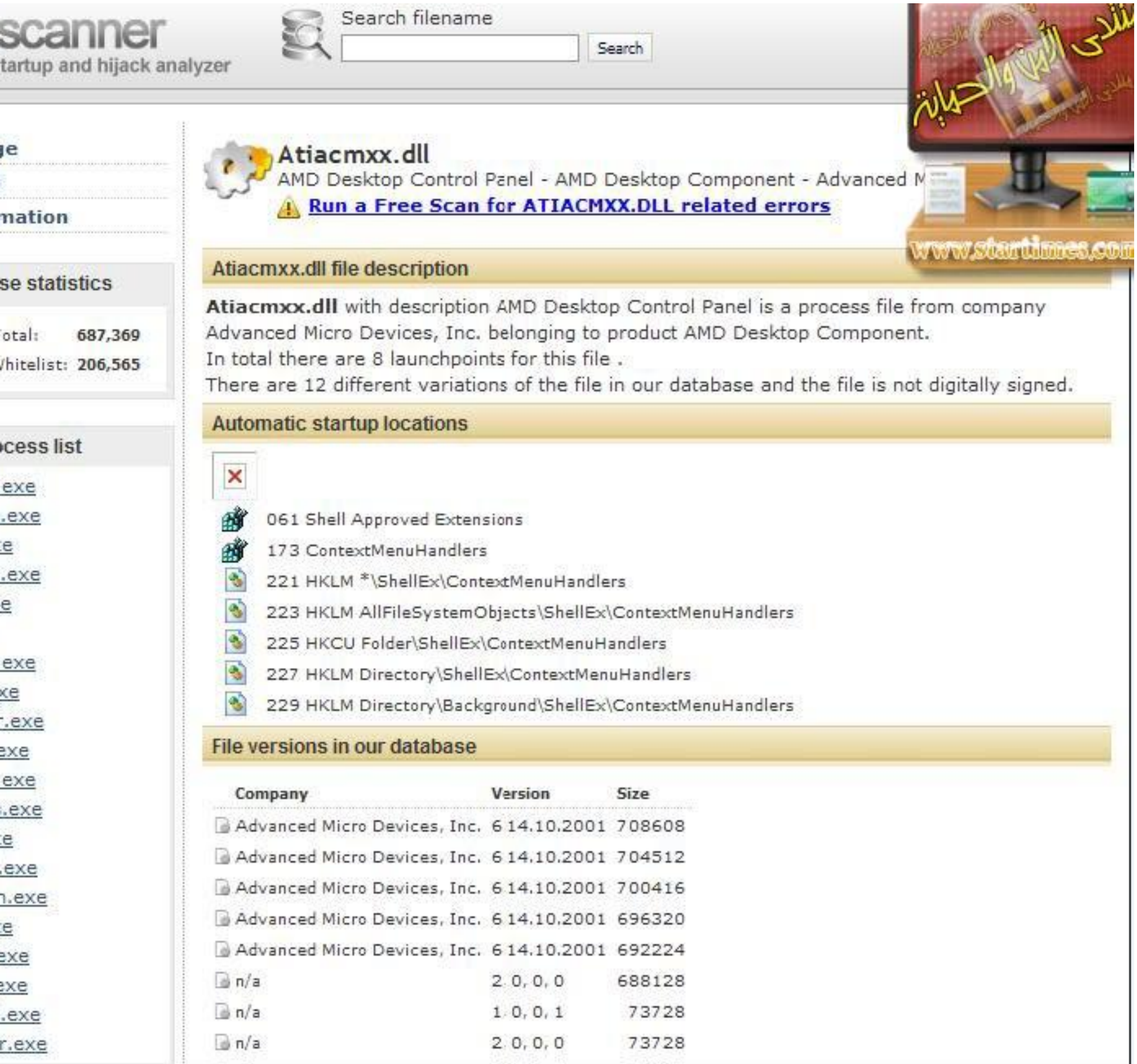
وهي موقع الأداة وهو

Lookup at Run scanner.net

عندما نضغط عليه يتم تحويلنا مباشرة الى الموقع

وهدا فحص للأحد الأسطر

هنا نجد جميع المعلومات المتعلقة بالسطر الدى أردنا فحصه



بنسبة للفحص بواسطة القيمة التشفيريةMD5

Lookup MD5 at FileAdvisor

لقد سبق وشرحتها بهذا الموضوع

☼◄ القيمة التشفيرية MD5 على ◄☼Runscanner

شرح القيمة التشفيرية MD5 على Runscanner

وتعتبر هده القيمة هي أكثر استعمالا في العديد من الأمور الأمنية خاصة كلمات المرور

وقواعد البيانات الى أخره ...اسمها العلمى هوData integrity

هي عبارة عن أرقام وحروف مشفرة طول مخرجات التشفير ب MD5 هو Bits128

لكن طول الرسالة الأصلية هو Bits 521 وادا زادت يتم تقسيمها الى حزمات هدا هو الدى يعطي لهده القيمة مصداقية.

كان هدا فقط نظرة عن هده القيمة

الأن نعود الى موضوعنا وهو كيفية استخراج هده القيمة بRunscanner

ثم فحصها على أحد المواقع الخاصة بالفحص

بعد عمل فحص للجهاز بواسطة Runscanner

يعطينا الكثير من الأسطر وادا شككنا فى أحد الأسطر على انها فيروسات

نقوم بالضغط عليها بيمين الفأرة ثم نختارLookup Md5 at FileAdvisor



بعد الضغط يتم تحويلنا الى الموقع الدي يكشف لنا عن القيمة



بعدما حصلنا عن القيمة ندخل على أحد مواقع الفحص

سأختار موقعvirustotal

http://www.virustotal.com

بعد الدخول على الموقع نقوم بتالى



هده هي نتيجة الفحص لسطر سليم



Antivirus	Version	Last Update	Result
hnLab-V3	2010.09.07.00	2010.09.07	-
ntiVir	8.2.4.50	2010.09.06	-
ntiy-AVL	2.0.3.7	2010.09.03	-
uthentium	5.2.0.5	2010.09.06	-
vast	4.8.1351.0	2010.09.06	-
vast5	5.0.594.0	2010.09.06	-
VG	9.0.0.851	2010.09.06	-
itDefender	[illegible]	2010.09.07	-
AT-QuickHeal	[illegible]	10.09.06	-
lamAV	[illegible]	0.09.07	-
omodo	[illegible]	9.07	-
rWeb	[illegible]	07	-
msisoft	[illegible]	9.07	-
Safe	[illegible]	09.05	-
Trust-Vet	[illegible]	.09.06	-
-Prot	[illegible]	2010.09.01	-
-Secure	9.0.15370.0	2010.09.07	-
ortinet	4.1.143.0	2010.09.05	-
Data	21	2010.09.07	-

وهده النتيجة مثال لسطر مصاب



0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

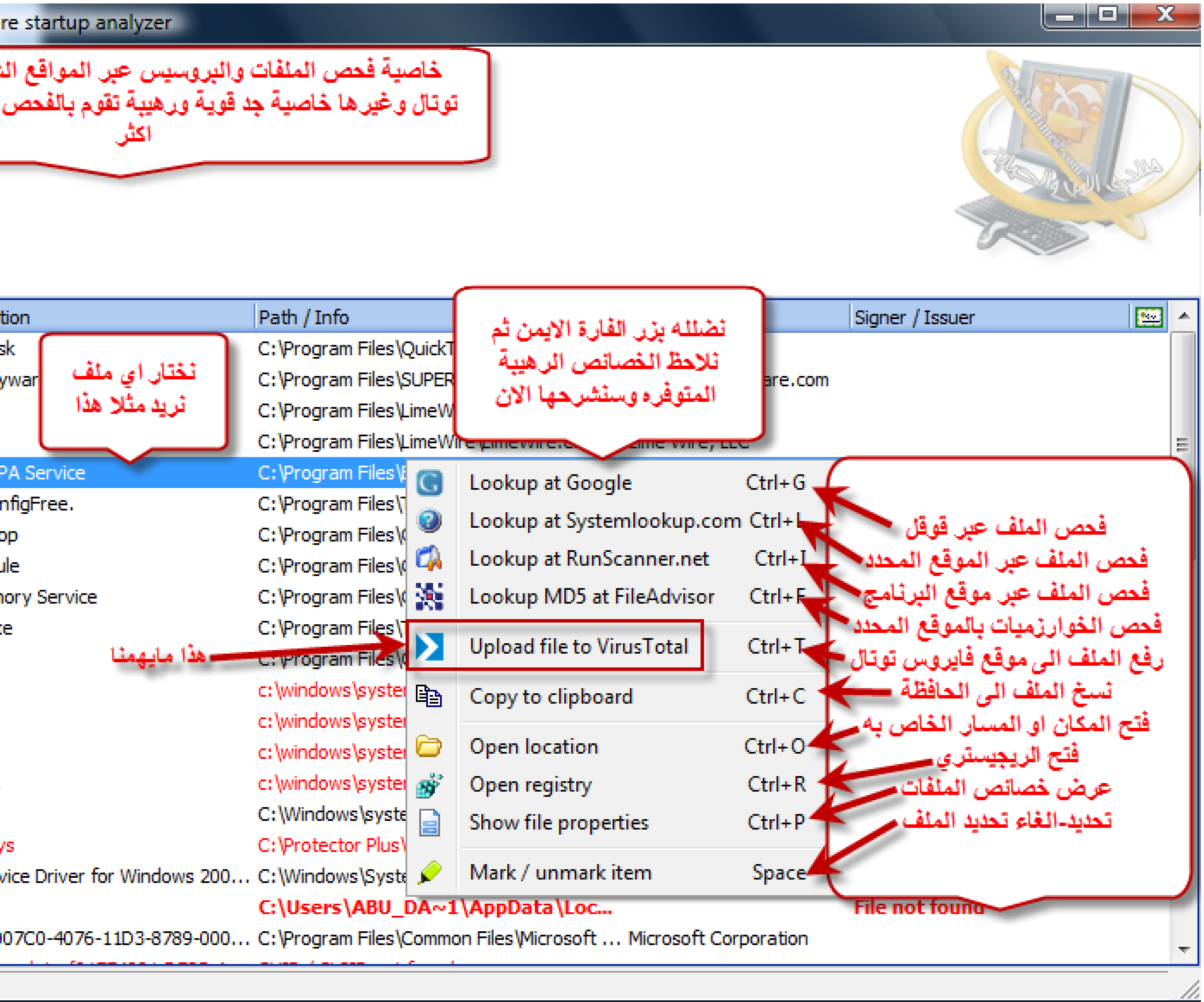
File name:	PIC675799074533-JPG-www.facebook.com.ex.vir
Submission date:	2010-09-10 20:49:01 (UTC)
Current status:	finished
Result:	27 /43 (62.8%)

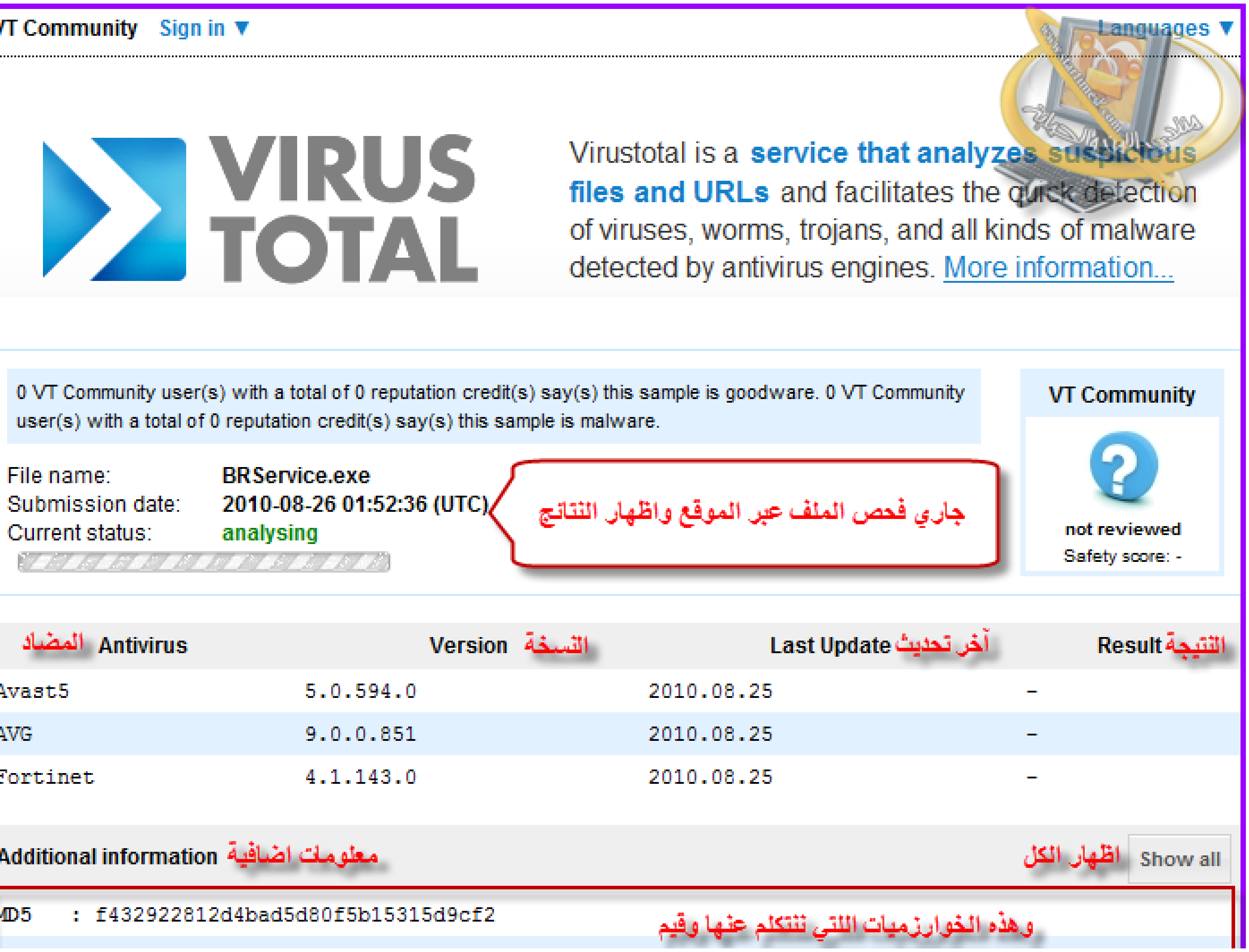
Compact

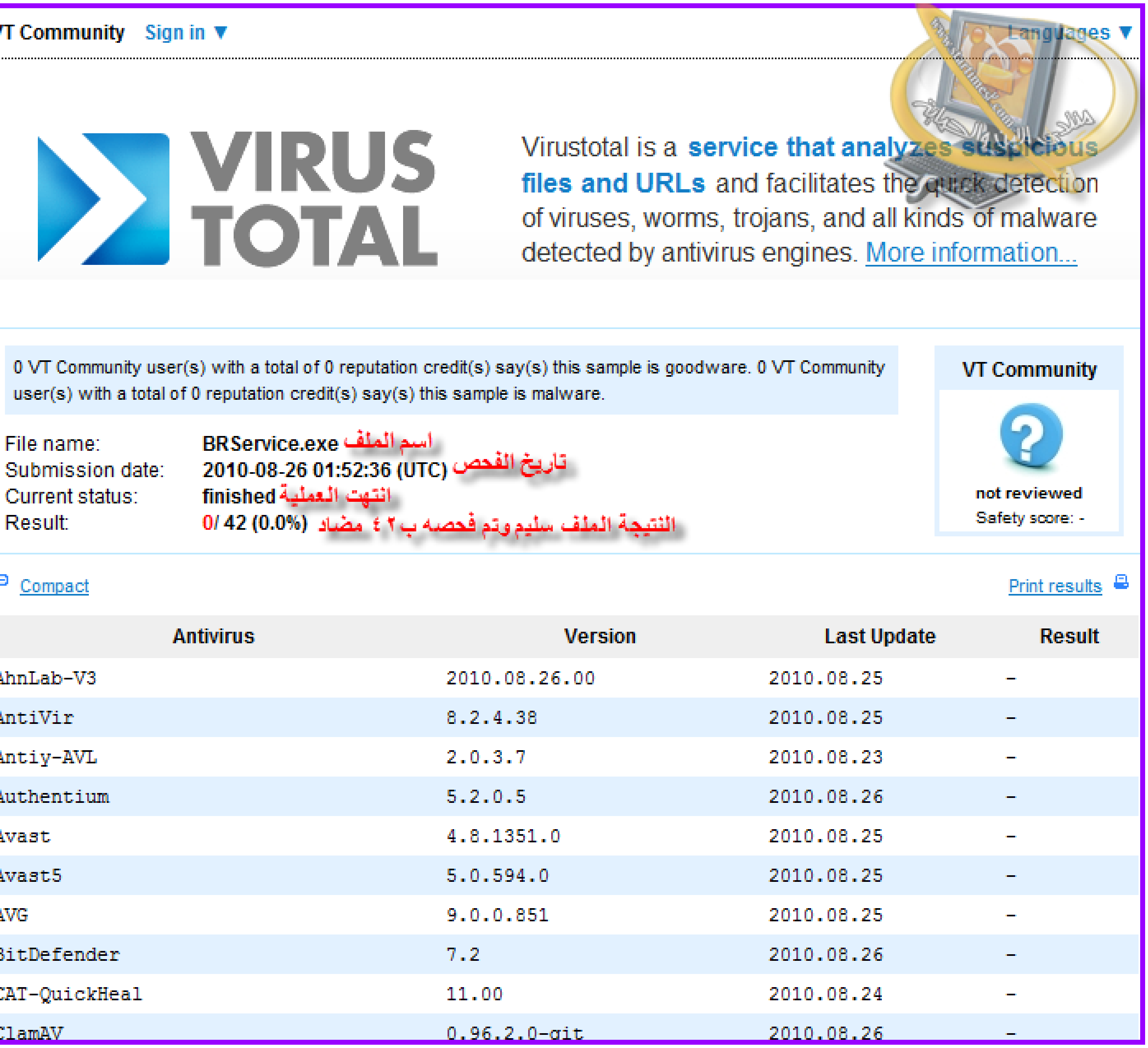
Antivirus	Version	Last Update	Result
nnLab-V3	2010.09.10.01	2010.09.10	Win32/Yahos.worm.68096
ntiVir	8.2.4.50	2010.09.10	Worm/IM.VB.AR
ntiy-AVL	2.0.3.7	2010.09.10	-
uthentium	5.2.0.5	2010.09.10	-
vast	4.8.1351.0	2010.09.10	Win32:Rootkit-gen
vast5	5.0.594.0	2010.09.10	Win32:Rootkit-gen
VG	9.0.0.851	2010.09.10	VB.AHIL
itDefender	7.2	2010.09.10	Win32.Worm.IM.VB.AR
AT-QuickHeal	11.00	2010.09.10	I-Worm.Yahos.ck
lamAV	0.96.2.0-git	2010.09.10	-
omodo	6036	2010.09.10	-
rWeb	5.0.2.03300	2010.09.10	Win32.HLLW.Siggen.1509
msisoft	5.0.0.37	2010.09.10	IM-Worm.Win32.Yahos!IK
Safe	7.0.17.0	2010.09.07	-
Trust-Vet	36.1.7846	2010.09.10	Win32/Pushbot.WI
-Prot	4.6.1.107	2010.09.01	-
-Secure	9.0.15370.0	2010.09.10	Win32.Worm.IM.VB.AR
ortinet	4.1.143.0	2010.09.10	-
Data	21	2010.09.10	Win32.Worm.IM.VB.AR

شرح خاصية رفع الملفات عبر موقعvirustotal

وهدا شرح للأخ عوض نتمنى ان تدعو له بشفاء


re startup analyzer
خاصية فحص الملفات والبروسيس عبر المواقع
توتال وغيرها خاصية جد قوية ورهيبة تقوم بالفحص
اكثر
Path / Info
Signer / Issuer
نختار اي ملف
نريد مثلا هذا
نضلله بزر الفارة الايمن ثم
نلاحظ الخصائص الرهيبة
المتوفره وسنشرحها الان
Lookup at Google Ctrl+G
Lookup at Systemlookup.com Ctrl+L
Lookup at RunScanner.net Ctrl+I
Lookup MD5 at FileAdvisor Ctrl+F
Upload file to VirusTotal Ctrl+T
Copy to clipboard Ctrl+C
Open location Ctrl+O
Open registry Ctrl+R
Show file properties Ctrl+P
Mark / unmark item Space
هذا مايهمنا
فحص الملف عبر قوقل
فحص الملف عبر الموقع المحدد
فحص الملف عبر موقع البرنامج
فحص الخوارزميات بالموقع المحدد
رفع الملف الى موقع فايروس توتال
نسخ الملف الى الحافظة
فتح المكان او المسار الخاص به
فتح الريجيستري
عرض خصائص الملفات
تحديد-الغاء تحديد الملف
C:\Users\ABU_DA~1\AppData\Loc...
File not found


VT Community
Sign in ▼
Languages ▼
VIRUS TOTAL
Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...
0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.
VT Community
not reviewed
Safety score: -
File name: BRService.exe
Submission date: 2010-08-26 01:52:36 (UTC)
Current status: analysing
جاري فحص الملف عبر الموقع واظهار النتائج
المضاد Antivirus
Version النسخة
Last Update آخر تحديث
Result النتيجة
Avast5 5.0.594.0 2010.08.25 -
AVG 9.0.0.851 2010.08.25 -
Fortinet 4.1.143.0 2010.08.25 -
Additional information معلومات اضافية
اظهار الكل Show all
MD5 : f432922812d4bad5d80f5b15315d9cf2
وهذه الخوارزميات اللتي نتكلم عنها وقيم



T Community Sign in ▼ Languages ▼

VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

VT Community

not reviewed
Safety score: -

File name: BRService.exe اسم الملف
Submission date: 2010-08-26 01:52:36 (UTC) تاريخ الفحص
Current status: finished انتهت العملية
Result: 0/ 42 (0.0%) النتيجة الملف سليم وتم فحصه ب ٤٢ مضاد

Compact Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.08.26.00	2010.08.25	-
AntiVir	8.2.4.38	2010.08.25	-
Antiy-AVL	2.0.3.7	2010.08.23	-
Authentium	5.2.0.5	2010.08.26	-
Avast	4.8.1351.0	2010.08.25	-
Avast5	5.0.594.0	2010.08.25	-
AVG	9.0.0.851	2010.08.25	-
BitDefender	7.2	2010.08.26	-
CAT-QuickHeal	11.00	2010.08.24	-
ClamAV	0.96.2.0-git	2010.08.26	-

وكدلك يمكننا الفحص عبر محرك البحثGoogle

ودلك على الشكل التالى



اخواني هدا العمل دائما نقوم به فى الخاصية

Extra stuff

بمجرد تحديد الأسطر فى هده الخاصية مباشرة يتم نحديدها ختى فى الخاصيةMalware hunting



كيفية حدف الأسطر الضارة التى وجدنا بتقرير


eware startup analyzer
Extra stuff
Scan
Process killer
Installed software
Temara_M2
Path / Info
Issuer
خاصية Extra stuff
هي التي سنشتغل عليها
ثم
نقوم بفلتر لتقرير لتظهر لنا فقط الأسطر
المشكوك فيها
كما هو موضح
www.startimes.com
Temara_M2
2.0.0.50
08/09/2010 00:43:43
Administrator
Windows 7 Ultimate
7600
Arabe (Maroc)
181
C:\Windows
%SystemRoot%\System32\drivers\etc
127.0.0.1
0
هدا هو الجزء الأول من
التقرير
و توجد به معلومات حول
الجهاز
re de sessions Windows
d'exécution client-serveur
de démarrage de Windows
d'exécution client-serveur
s Services et Contrôleur
rity Authority Process
gestionnaire de session locale
d'ouverture de session Windows
Microsoft Corpora... Microsoft Windows : Microsof...
الجزء الثانى من التقرير
وهو خاص بالبروسيسات
ويجب فحصها

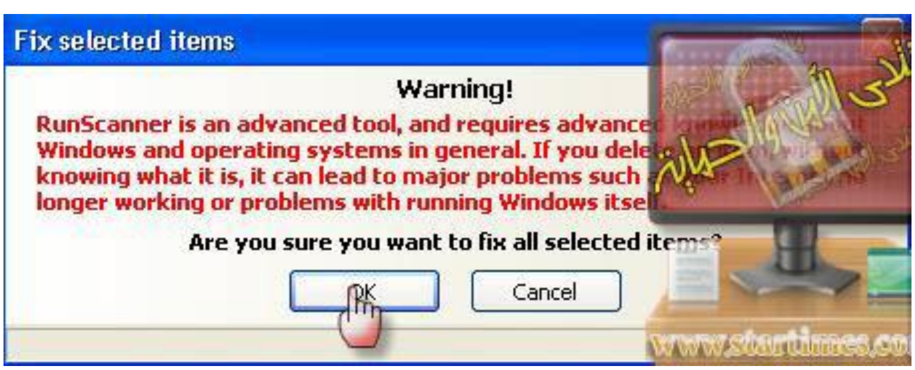


نتاكد من الأسطر التى أردنا حدفها ودلك


eware startup analyzer
Extra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Item fixer
Loaded modules
Temara_M2
Filter
items listed in this screen are not in our whitelist or the file doesn't exist.
t indicate that the file is malware or unwanted. Deleting a valid file can cause damage to your operating system.
www.startimes.com
Path / Info
Company
Signer / Issuer
C:\Program Files\Avira\AntiVir PersonalEd... Avira GmbH
Premium MailGuard
Avira AntiVir Premium
Premium Guard
Premium WebGuard
File not found
C:\WINDOWS\system32\drivers\PQNTDr... PowerQuest Corporation
C:\WINDOWS\system32\DRIVERS\ssmdr... AVIRA GmbH
C:\WINDOWS\system32\drivers\WDICA....
fichage Panorama du Panne... deskpan.dll
extension {B41DB860-8EE4... C:\Program Files\WinRAR\rarext.dll
ما علينا سوى الضغط على
Malware hunting
ثم
Item fixer
لكي تظهر لنا الأسطر التى يجب حدفها



نضغطOk

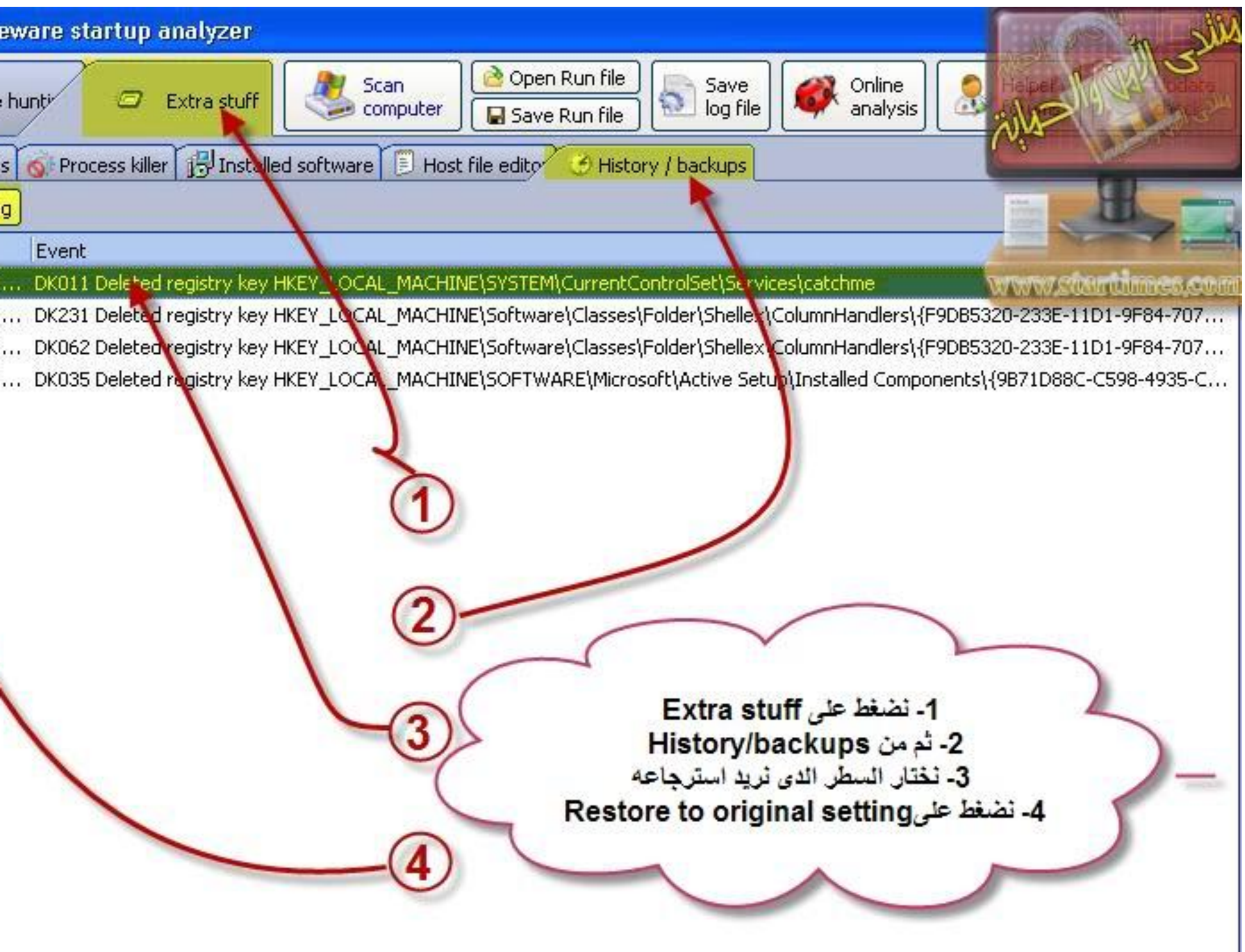


ثم Ok لتأكيد



الأن مع

شرح لكيفية استرجاع الأسطر التى تم حدفها بالخطأ



ثم نضغط على

Yes

لتأكيد



العملية تمت بنجاح



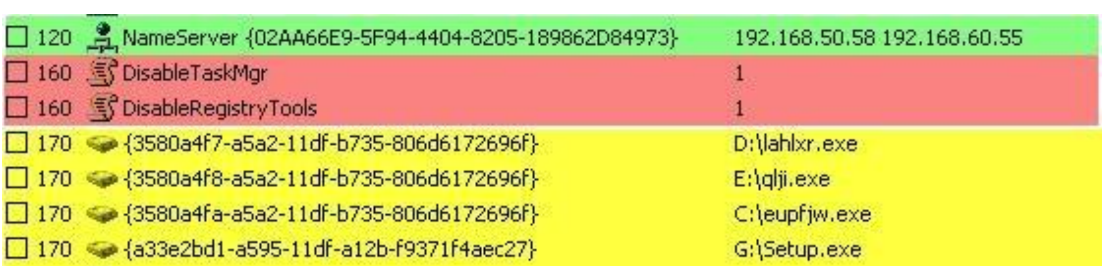
اخواني أعتقد يجب علينا الوقوف هنا
حتى لا نبتعد كثيراا على الأعضاء اللدين لم يحضور الدرس
+المحور القادم فهو يريد التركيز
لأنه سنقوم فيه بمقارنة أسطر hijackthis مع أسطر Runscanner
وكيفية معرفة بعض الأسطر التى تظهر بشكل واضح على هيجاكديس
وبشكل معقد علىRunscanner

فقط لدي اضافة او تعقيب اعتقد ان اكبر شيء يجب على اداة ال RUNSCANNER تجاوزه هي قضية MD5فيفضل ان نجد النتيجة مباشرة من احد المواقع دون المرور على الفيروس توتال او غوغل لانو الموقع المستعمل حاليا يحتاج للتسجيل به اي لا اهمية له سوى معرفة MD5 للملفات وهذه العملية يمكن ان تقوم بها الاداة بدون مواقع مثل ما تقوم به اداة الهيجاك...

نعم أخي فكرة جيدة

بنسبة للأمتداد مثلا هده الأسطر الملونة بالأصفر فهي لا تحتاج الى فحص

فهي مباشرة للحدف



120	NameServer {02AA66E9-5F94-4404-8205-189862D84973}	192.168.50.58 192.168.60.55
160	DisableTaskMgr	1
160	DisableRegistryTools	1
170	{3580a4f7-a5a2-11df-b735-806d6172696f}	D:\lahlxr.exe
170	{3580a4f8-a5a2-11df-b735-806d6172696f}	E:\qlji.exe
170	{3580a4fa-a5a2-11df-b735-806d6172696f}	C:\eupfjw.exe
170	{a33e2bd1-a595-11df-a12b-f9371f4aec27}	G:\Setup.exe

جيد اخواني الأن بعد فتح الأداة وعمل تقرير

سنضغط علىExtra stuff

وبتالى سنواجه أولا فقرة وهي المثمثلة فى هده الصورة

والتى تعطينا معلومات على الجهاز



الأن سنتعرف من خلال Runscanner كيفية معرفة وجود الهوست بالجهاز

أي أسطر 01 التى نجدها فيhijackthis

مثل هده الأسطر

O1 - Hosts: 74.125.45.100 target=_new>www secure-plus-paymenom
O1 - Hosts: 74.125.45.100 target=_new>www getavplusnow com
O1 - Hosts: 74.125.45.100 safebrowsing-cache.google.com
O1 - Hosts: 74.125.45.100 urs.microsoft.com

بخصوص أداة Runscanner

الأمر سهل والصورة تبين دلك



الجميل هو ان الأداة يمكنها ان تتخلص من الهوست

الصور توضح كيفية التخلص منه


lyzer
ra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Installed softwar
Host file editor
History / backups
لكي نقضي على
o default



تفضل أخي لتتعرف على الهوست أكثر

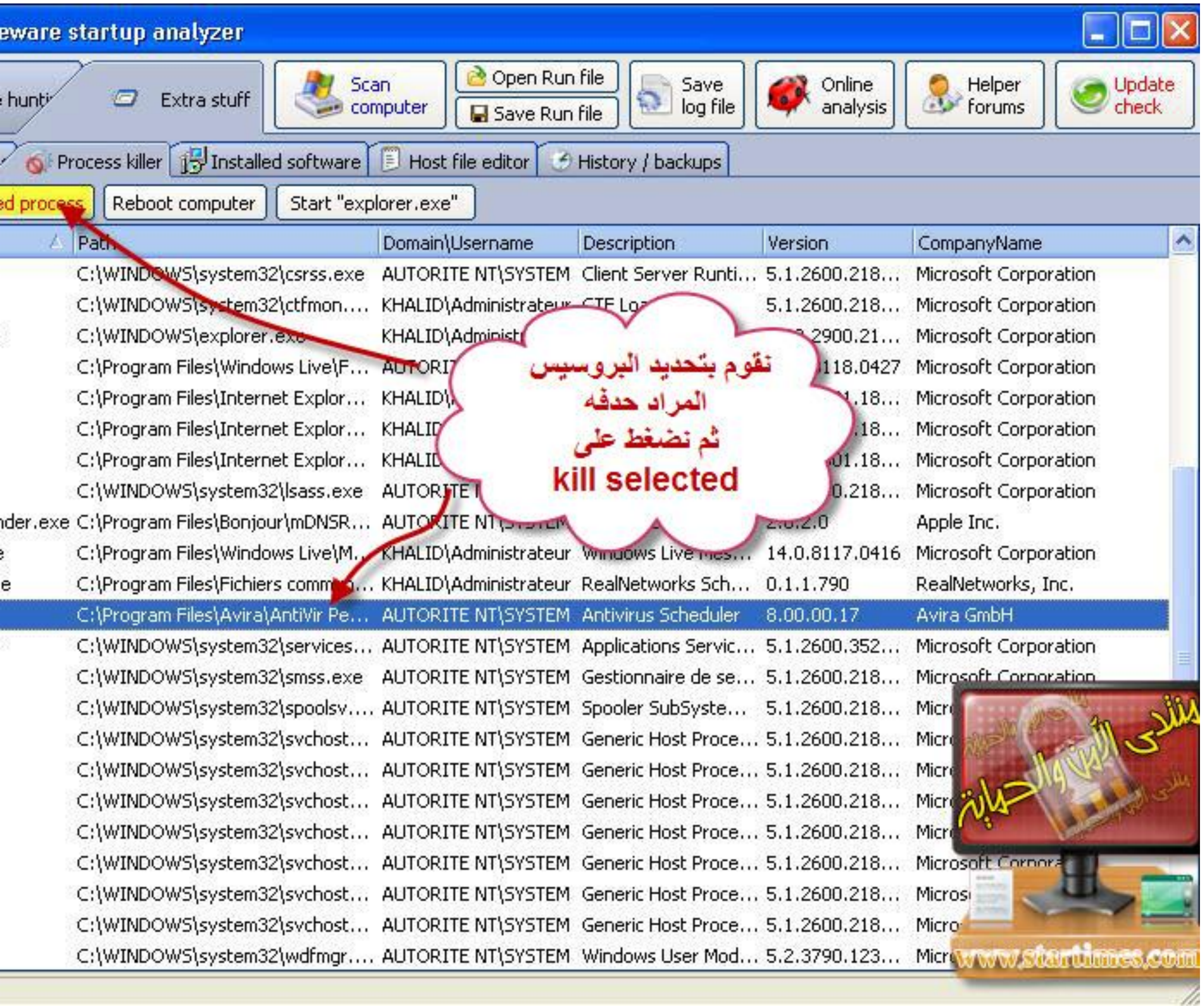
★ **درس حول التعــ© HOSTS ©ـــديل على**

الفقرة التانية وهي خاصة ب

البروسيسات الشغالة بالجهاز وهي الأخرى يجب فحصها جيدا!!!!



كيفية حدف البروسيسات



المرحلة التى تأتي بعد البروسيسات الشغالة

وهي البرامج التي تقلع مع تشغيل الونداوز

بنسبة للأسطر التي تقلع مع تشغيل الونداوز في هيجاك ديس تأخد الرقم04

لكن في runscanner الأمر مختلف وتوجد عدة طرق لمعرفتها

أولا بنسبة للخاصية Malware hunting تبدأ أرقام الاسطر التى تقلع مع بدأ تشغيل الونداوز من 002

مثلا في هده النسخة تبدأ من 002 الى 008 لكن هدا قد يختلف

فهده الصورة يتبين لنا أن الأسطر التى تقلع مع الجهاز هي 002 و 003 و 004



	Entry description	Path / Info	Company	Signer / Issuer
002	Adobe Reader Speed Launcher	C:\Program Files\Adobe\Reader 9.0\Rea...	Adobe Systems Incorpo...	
003	Z810PNP	C:\Program Files\Modem Samsung SCH-U...		
003	Z810SysStart	C:\Program Files\Modem Samsung SCH-U...		
003	AdobeUpdater	C:\Program Files\Fichiers communs\Adob...	Adobe Systems Incorpo...	
004	Notification de cadeaux MSN	C:\Documents and Settings\morad\Applic...	Microsoft Corporation	

لكن أنا أنصح بأن الطريقة الجيدة في معرفة الأسطر التى تقلع مع تشغيل الونداوز هي موجودة في خاصية Extra Stuff

لأنها تعطينا جميع البرامج والملفات التى تبدأ مع تشغيل الونداوز وسهل معرفتها

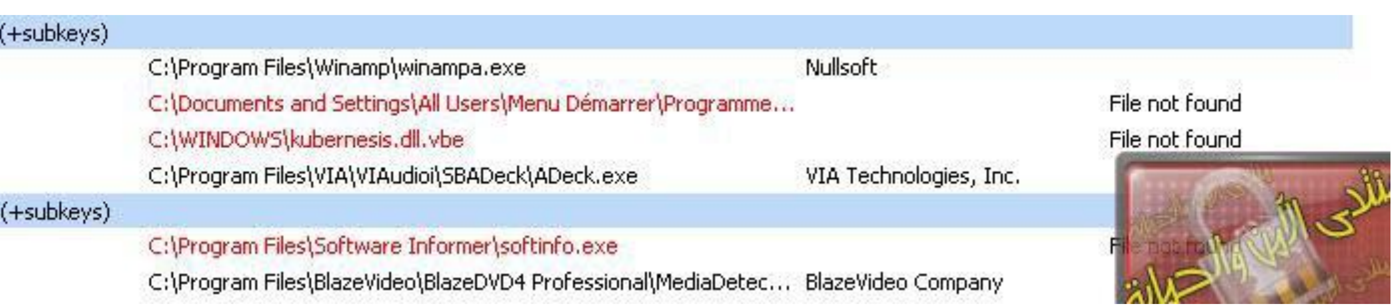
الصورة توضح سهولة هده الخاصية فقط يمكن معرفتها من خلال كلمة Run أو Démarrage وبتالى نتجاهل الارقام



بنسبة لبرامج التى تقلع مع تشغيل الونداوز
دائما نتجنب أسطر الويفي وبرنامج الحماية وجدار الناري
وأسطر موديم واللغة وأسطر النت وكدلك نترك البرامج التى نريدها ان تقلع مع تشغيل الجهاز
أما الاسطر التى نراها ملونة بالأحمر فهي مباشرة للحدف

هدا مثال للفيروس kubernesis.vbe

ونلاحظ بأن الاداة قامت بتوضيحه باللون الأحمر وهده ميزة جيدة للأداة



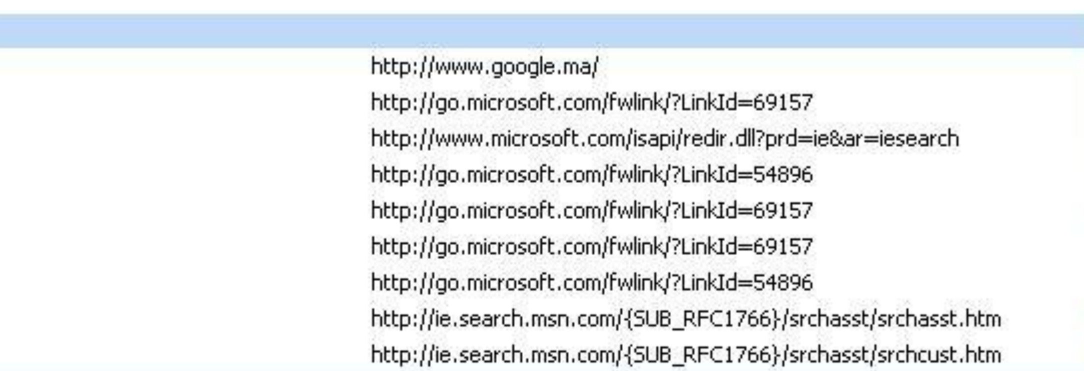
اخواني ادا كان كل شيئ واضح
سننتقل الى توضيح بعض أسطر hijackthiss
على أداة Runscanner
لأننى سبق وقرأة فى أحد النقاشات بالمنتدى
أن runscanner لا تحتوي على ما يوجد ب hijackthis
أي من خلال بعض الأسطر في hijackthis
نعرف أنا الجهاز مصاب
سأقول نعم حتى أداة runscanner تكتشف جميع أسطر hijackthis
فقط يجب البحث جيداا
وسأضع بعض الأمثلة

سنبدأ بأسطر R0 و R1

هده الأسطر خاصة بhijackthis

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://www.google.fr/
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/?LinkId=69157
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157

وعلى أداة runscanner نجدها على هدا الشكل دائما نتبع المسار



أما بخصوص أسطر 01 أي المتعلقة بالهوست لقد سبق وتطرقنا اليها

الأن سنري أسطر 07 في hijackthis وكيف تظهر علىrunscanner

عندما نجد العدد 1 فهدا يعنى أن Task manger مصاب أو بالفرنسيةgestionnaire des taches



أما

أسطر 06 فيhijackthis

تظهر على هدا الشكل فىrunscanner



بنسبة لبرامج التى تقلع مع تشغيل الونداوز
دائما نتجنب أسطر الويفي وبرنامج الحماية وجدار الناري

وأسطر موديم واللغة وأسطر النت وكدلك نترك البرامج التى نريدها ان تقلع مع تشغيل الجهاز
أما الاسطر التى نراها ملونة بالأحمر فهي مباشرة للحدف

بخصوص هده الأسطر اعتمد على

systemlookup.com

لقد قمت بشرحه بالدرس 2

بخصوص هده الاسطر عندما نجد القيمة 1 نقوم بخدفها



أما

عندما نجدها بتقريرنا مباشر للحدف



اخي لم تفهم قصدي جدا ومازلت تقول ان سطر الاحمر دائما للحدف سأقوم بتجربة على جهازي بحذف ملف explorer.exe موجود في مجلد نظام windows وساقوم

بوضع تقرير

يعني هذا ما جري من تغيرات عند حدف ملف **explorer.exe** من نظام لنفترض اننا حذفنا هذا سطر من روجيستري واردنا ان نحل مشكلة بنسخ ملف احتاطي للملف

explorer.exe ونسخناه في مجلد نظام مع العلم اننا حذفنا هذا السطر من روجيستري فهل سيشتغل ملف **explorer.exe** مرة اخي مع اشتغال النظام ؟!

أسطر **hijackthis** التي سبق وتوضيحها فى الدرس السابق وهي

01 , R0 , R1 , 07 , 06 ,

والأن مع أسطر **08**

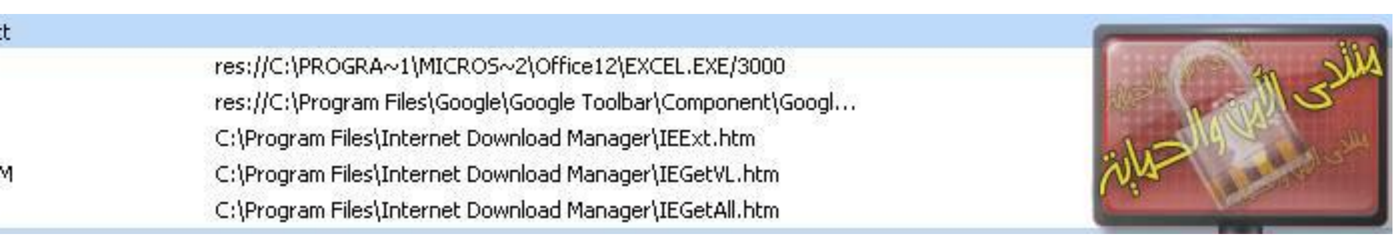
هده أمثلة لأسطر **08** في **hijackthis** أما على **runscanner** نجدها

فى الخاصيتين أي **Malware hunting** و**Extra stuff**

هده الصور على الخاصية **Malware hunting**



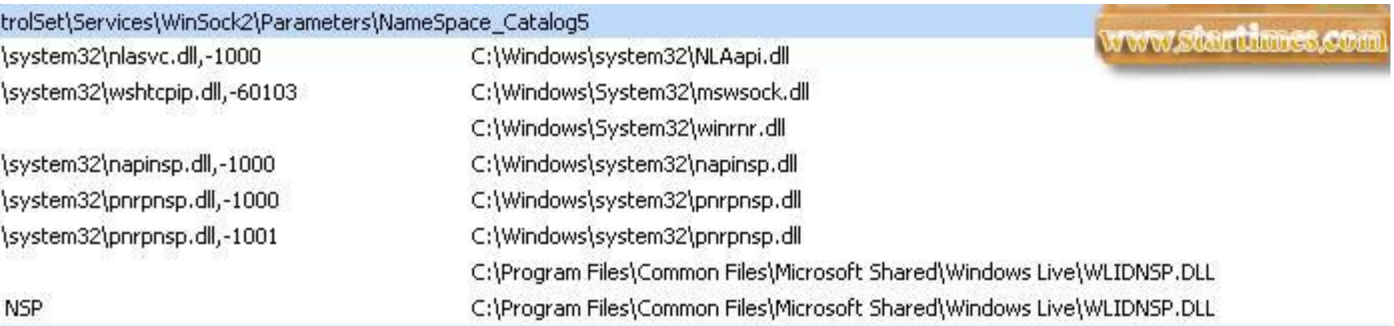
وهده على الخاصية**Extra stuff**



بنسبة لهده الأسطر يجب فحصها

أو النظر فيها ادا عرفنا البرامج التى تعود فلابأس بتركها وادا لم نعرف دلك يجب فحصها

أسطر 10 على hijckathis أما على Runscanner نجدها على هدا الشكل



trolSet\Services\WinSock2\Parameters\NameSpace_Catalog5	
\system32\nlasvc.dll,-1000	C:\Windows\system32\NLAapi.dll
\system32\wshtcpip.dll,-60103	C:\Windows\System32\mswsock.dll
	C:\Windows\System32\winrnr.dll
\system32\napinsp.dll,-1000	C:\Windows\system32\napinsp.dll
\system32\pnrpnsp.dll,-1000	C:\Windows\system32\pnrpnsp.dll
\system32\pnrpnsp.dll,-1001	C:\Windows\system32\pnrpnsp.dll
	C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDNSP.DLL
NSP	C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLIDNSP.DLL

الأسطر المهمة التى لا يجب حدفها هي التى تنتهي ب

mswsock.dd

winrnr.dl

pnrpnsp.dll

وهنا يجب حدف السطريين الأخيرين وهما

WLIDNSP.DLL

وكدلك يمكن الاعنماد على هدا الموضوع فى اصلاح هدا الخلل والدي يتعلق بالاتصال

http://www.startimes.com/f.aspx?t=25076006

أسطر015 في hijackthis نجدها على الشكل التالى بنسبة لRunscanner

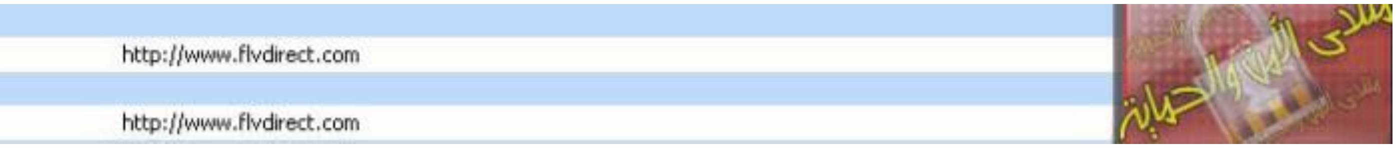
هده بنسبة للخاصيةMalware hunting



http://www.flvdirect.com
http://www.flvdirect.com



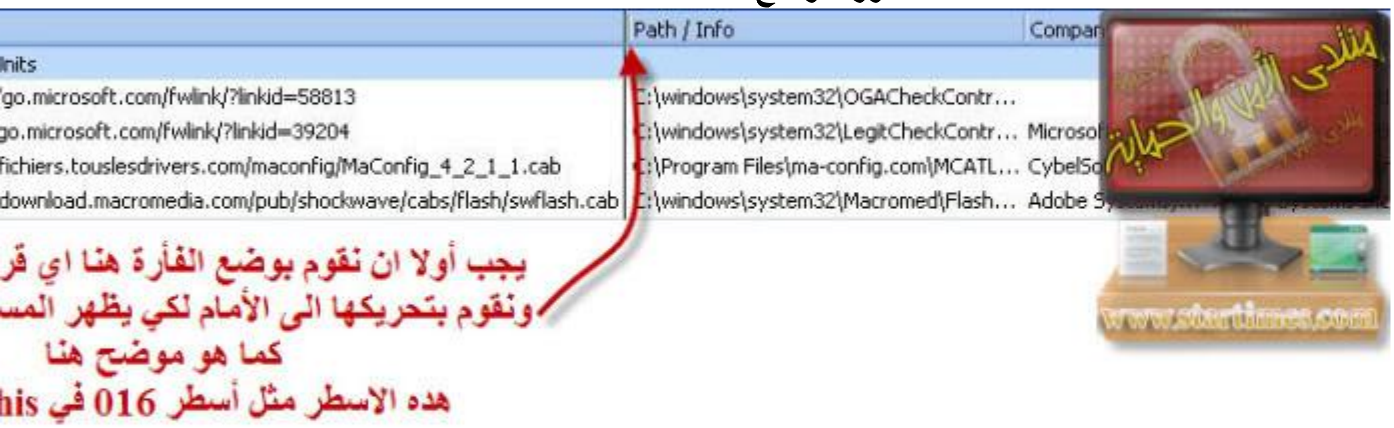
وهده لخاصيةExtra stuff



أسطر016 في hijackthis

أما على Runscanner نجدها في خاصية Extra Stuff هده الخاصية نجد فيها كل شيأ وهدا جيد

الصورة توضح دلك

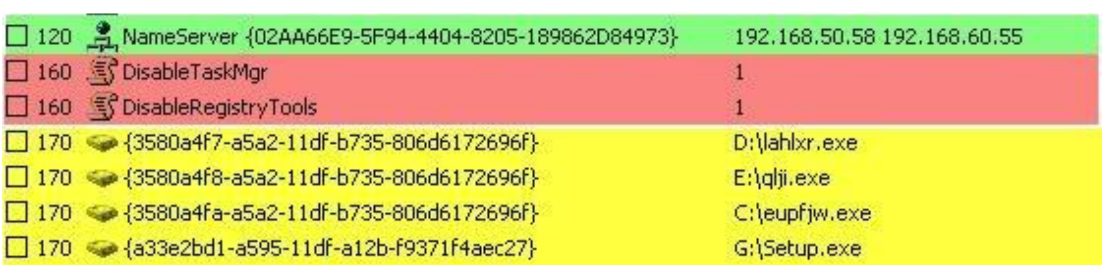


هدا مثال لسطر 017 الموجد في hijackthis

في هيجاك ديس يكون على هدا الشكل

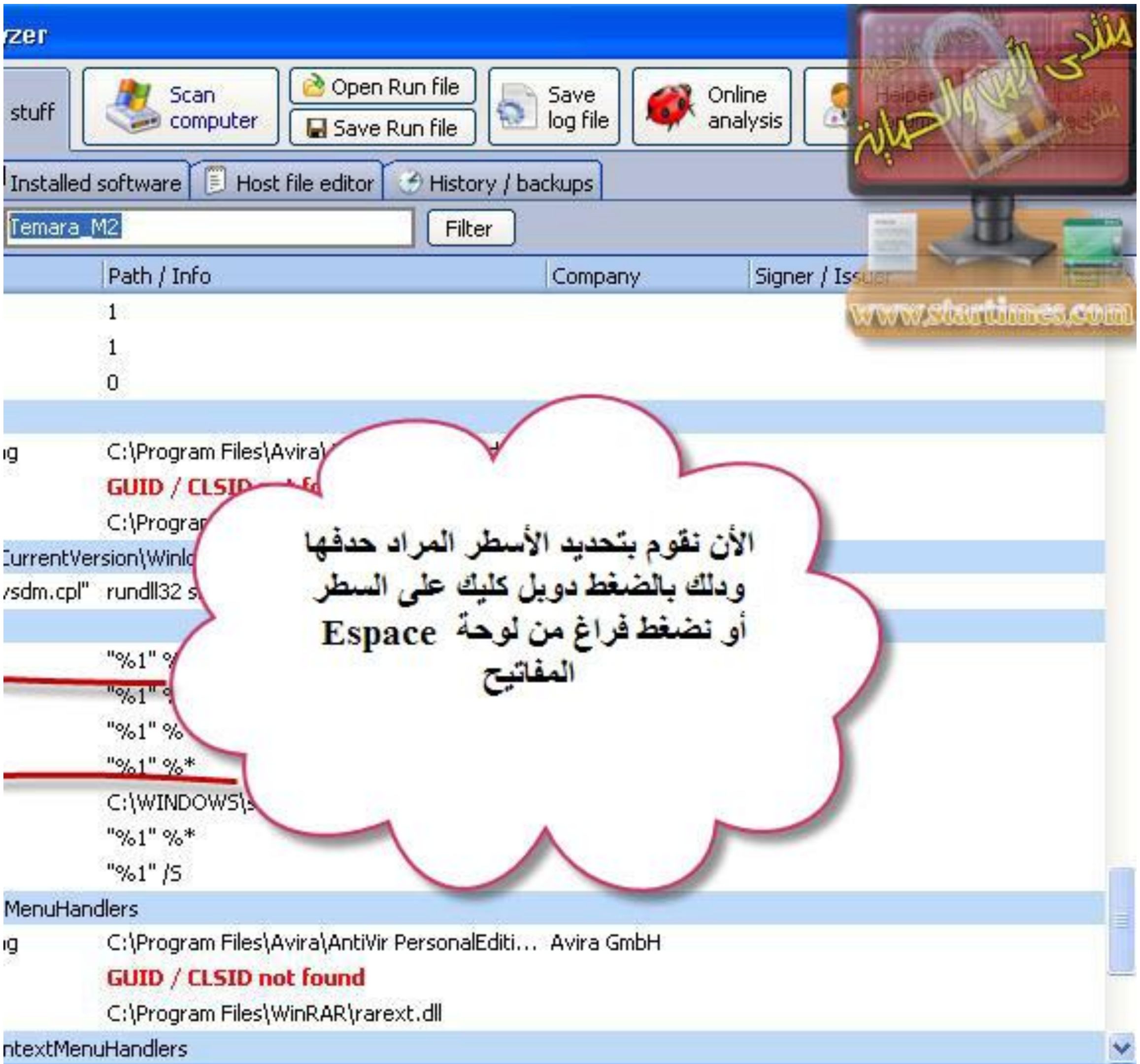
O17 - HKLM\System\CCS\Services\Tcpip\..\{02AA66E9-5F94-4404-8205-189862D84973}: NameServer = 192.168.50.58 192.168.60.55

أما في Runscanner هو السطر الملون بالأخضر



120	NameServer {02AA66E9-5F94-4404-8205-189862D84973}	192.168.50.58 192.168.60.55
160	DisableTaskMgr	1
160	DisableRegistryTools	1
170	{3580a4f7-a5a2-11df-b735-806d6172696f}	D:\lahlxr.exe
170	{3580a4f8-a5a2-11df-b735-806d6172696f}	E:\qlji.exe
170	{3580a4fa-a5a2-11df-b735-806d6172696f}	C:\eupfjw.exe
170	{a33e2bd1-a595-11df-a12b-f9371f4aec27}	G:\Setup.exe

كيفية حدف الأسطر بعد تحديدها



ا

ثم نضغط علىMalware hunting

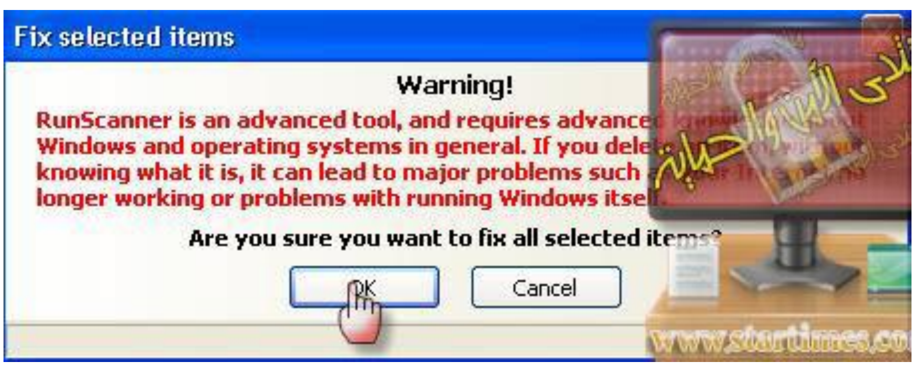
ثم

item fixer

ثم



نضغطOk



ثم Ok لتأكيد



ليست للحدف فقط ولحد الأن يوجد فيروس واحد يتضح من خلال هده الأسطر وهو للحدف

وهو

NameServer = 85.255.115.2,85.255.112.7

عندما نجد مثل هده الأرقام المهم ان تكون تبدأ ب 85.225

فهدا مباشرة للحدف

كيفية فحص تقرير وتحديد أسطره

ادا أرسله لنا أحد الأعضاء

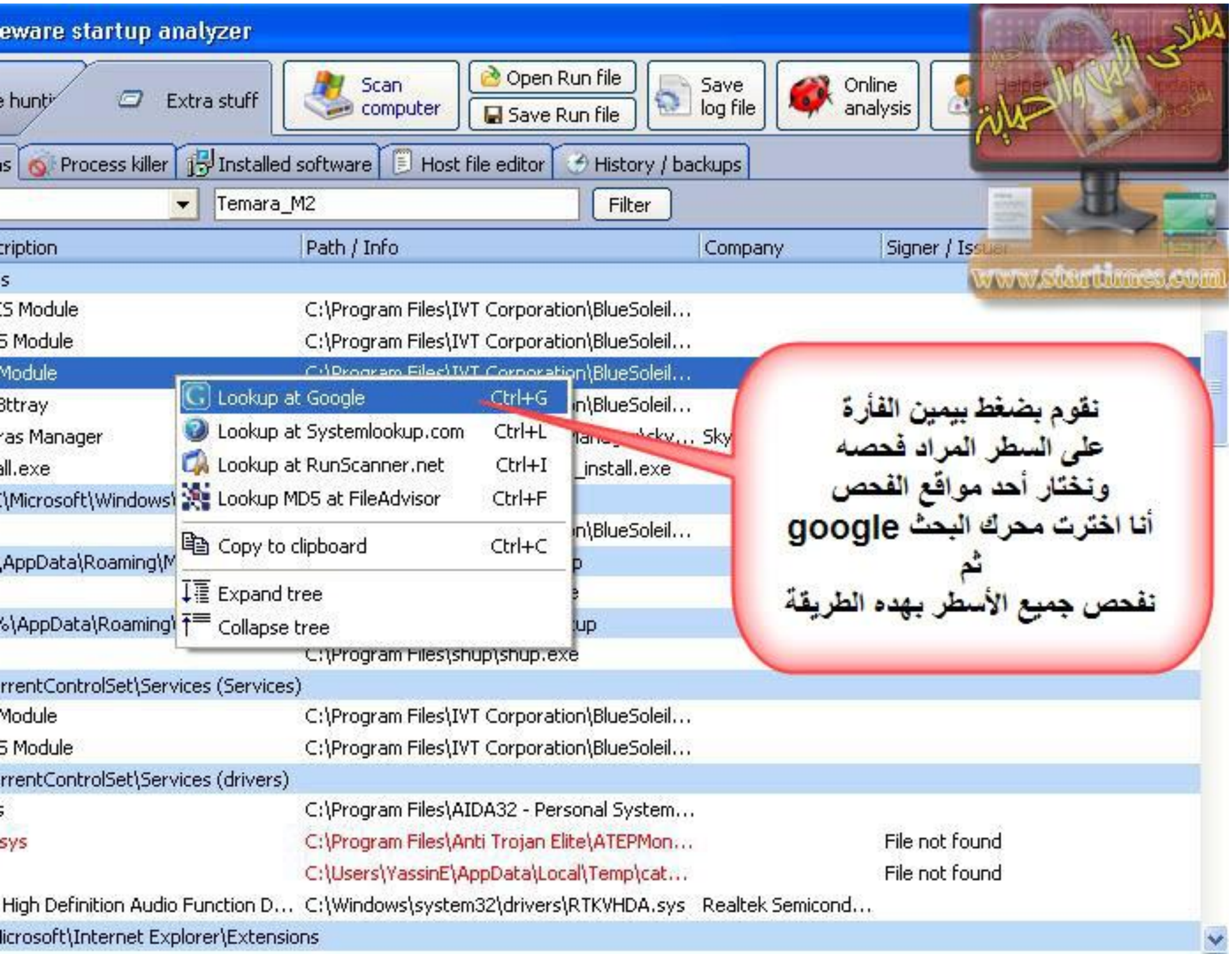
والتقرير الدى نعتمد عليه يجب ان يكون بصيغة run وليس log

نتابع الشرح بالصور




eware startup analyzer
hunting
Extra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Item fixer
Loaded modules
Temara_M2
Filter
tems listed in this screen are not in our whitelist or the file doesn't exist.
t indicate that the file is malware or unwanted. Deleting a valid file can cause damage to your operating system.
www.startimes.com
هده هي واجهة التقرير
عندما نضغط دوبل كليك على التقرير
مباشرة تظهر لنا هده الواجهة


eware startup analyzer
Extra stuff
Scan computer
Process killer
Installed software
Temara_M2
Path / Info
Issuer
www.startimes.com
خاصية Extra stuff
هي التي سنشتغل عليها
ثم
نقوم بفلتر لتقرير لتظهر لنا فقط الأسطر
المشكوك فيها
كما هو موضح
Temara_M2
2.0.0.50
08/09/2010 00:43:43
Administrator
Windows 7 Ultimate
7600
Arabe (Maroc)
181
C:\Windows
%SystemRoot%\System32\drivers\etc
127.0.0.1
0
هدا هو الجزء الأول من
التقرير
و توجد به معلومات حول
الجهاز
re de sessions Windows
d'exécution client-serveur
de démarrage de Windows
d'exécution client-serveur
s Services et Contrôleur
rity Authority Process
gestionnaire de session locale
d'ouverture de session Windows
Microsoft Corpora... Microsoft Windows : Microsof...
الجزء الثانى من التقرير
وهو خاص بالبروسيسات
ويجب فحصها


eware startup analyzer
Extra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Process killer
Installed software
Host file editor
History / backups
Temara_M2
Filter
Path / Info
Company
Signer / Issuer
Lookup at Google Ctrl+G
Lookup at Systemlookup.com Ctrl+L
Lookup at RunScanner.net Ctrl+I
Lookup MD5 at FileAdvisor Ctrl+F
Copy to clipboard Ctrl+C
Expand tree
Collapse tree
نقوم بضغط بيمين الفأرة
على السطر المراد فحصه
ونختار أحد مواقع الفحص
أنا اخترت محرك البحث google
ثم
نفحص جميع الأسطر بهده الطريقة
www.startimes.com



eware startup analyzer
Extra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Process killer
Installed software
Host file editor
History / backups
Temara_M2
Filter
Path / Info
Company
www.startimes.com
withoutlogon
noutlogon
gistryTools
ontextMenuHandlers
nsion for Malware scanning
GUID / CLSID not found
SSES_ROOT batfile
SSES_ROOT cmdfile
SSES_ROOT comfile
SSES_ROOT exefile
SSES_ROOT htafile
SSES_ROOT piffile
SSES_ROOT scrfile
lasses*\ShellEx\ContextMenuHandlers
C:\Program Files\Avira\AntiVir PersonalEditi... Avira GmbH
C:\Program Files\WinRAR\rarext.dll
lasses\Folder\ShellEx\ContextMenuHandlers
الأن نقوم بتحديد الأسطر المراد حدفها
ودلك بالضغط دوبل كليك على السطر
أو نضغط فراغ من لوحة Espace
المفاتيح





هدا هو التقرير الدي تم تحليله من طرف الخبير
فقط يجب ارسال التقرير للعضو لكي يقوم
بحدف الأسطر
التى تم تحديدها بالتقرير

****

ملاحظة: الخبير لا يستطيع حدف الأسطر فقط يقوم بتحديدها ويحفظ التقرير

ويرسله لصاحبه لكي يقوم بالحدف لأنه هو الدى يمتلك خاصية الحدف

وعملية الحدف التى يجب على صاحب التقرير القيام بها

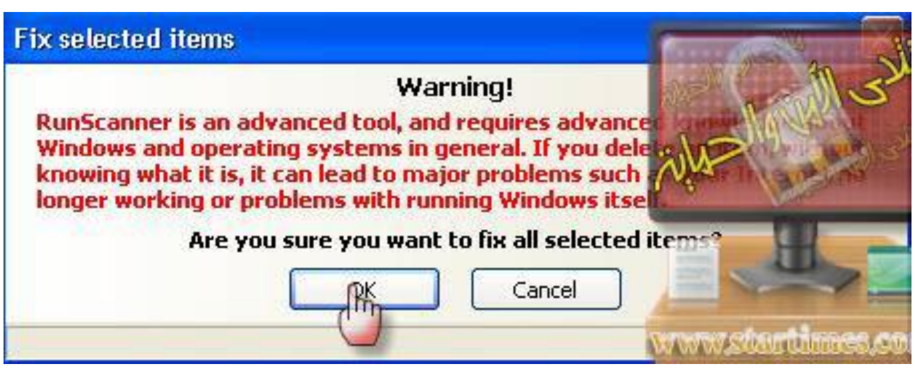
هي على الشكل التالى




ما علينا سوى الضغط على
Malware hunting
ثم
Item fixer
لكي تظهر لنا الأسطر التى يجب حدفها
eware startup analyzer
Extra stuff
Scan computer
Open Run file
Save Run file
Save log file
Online analysis
Item fixer
Loaded modules
Temara_M2
Filter
items listed in this screen are not in our whitelist or the file doesn't exist.
t indicate that the file is malware or unwanted. Deleting a valid file can cause damage to your operating system.
Path / Info
Company
Signer / Issuer
File not found
www.startimes.com



نضغط Ok



ثم Ok لتأكيد



هدا البرنامج للأخوة اللدين لا يعرفون كيفية رفع التقارير

برنامج خفيف للرفع التقارير

وهوShup

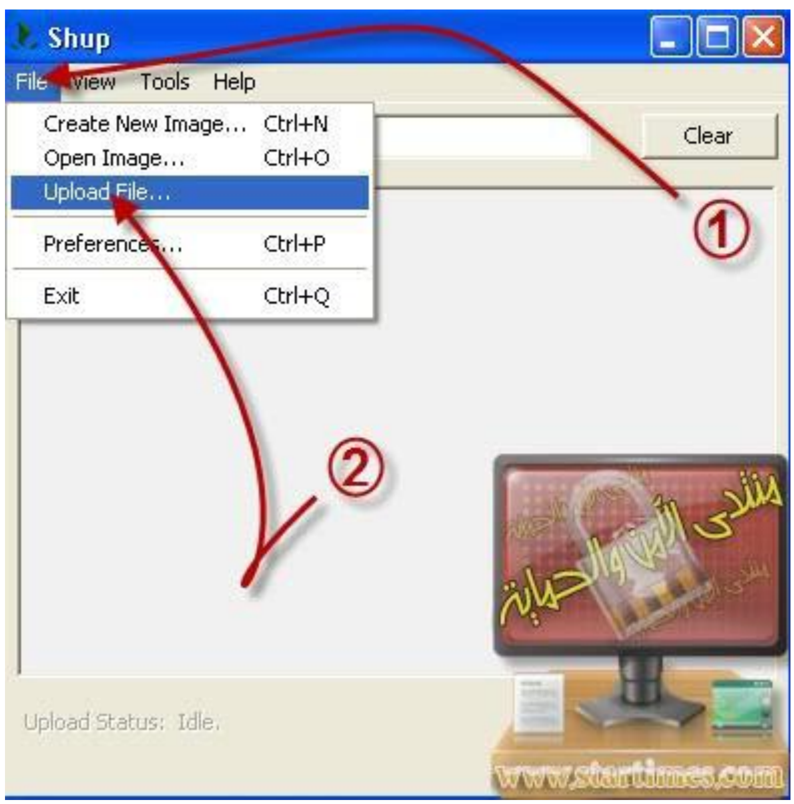
هدا موقع البرنامج

http://shup.com/

من هنا تحميل البرنامج

Shup v0.27 (692kb)

لرفع نقوم بتالى




Ouvrir
Regarder dans :
Bureau
Mes documents récents
Bureau
Mes documents
Poste de travail
Favoris réseau
runscanner
runscanner
runscanner Rapport Reda
runscanner reda
نختار الملف الذي نريد
رفعه ثم
نضغط Ouvrir
أنا قمت برفع أحد
التقارير بصيغة
run
www.startimes.com
Nom du fichier :
runscanner Rapport Reda
Fichiers de type :
All Files
Ouvrir en lecture seule
Ouvrir
Annuler


Shup
File
View
Tools
Help
Search
Clear
runscanner-Rapport-Reda.run
2010-09-07
http://shup.com/Shup/4136
Open with default app
Open in Shup
Open with default browser
Open containing folder
Copy URL
Copy file path
Copy with custom formatting...
Remove from history
Delete local file
Upload
كليك بيمين الفأرة
ثم نختار
Copy URL
Upload Status: Idle...

ثم نقوم بلصقه للخبير الدي سيقوم بفحص التقرير

ايوب "محب العطاء"

اتمنى ان تدعوا لي بالنجاح في دراستي